Annual Academic Sessions 2011
ISSN 2012-9912; ©2011 Open University of Sri Lanka

CYBER CRIMES IN SRI LANKAN PERSPECTIVE

M. K. Goonathilaka*

Department of Legal Studies, Open University of Sri Lanka

INTRODUCTION

With the expansion of the use of computers Internet also has become a vital communication tool in today's life. The wider use of Internet not only brought benefits to the society but also exposed the society to new breeds of threats and hacking offences. Internet related crimes are generally called Cyber Crimes. To combat Cyber Crimes the Sri Lankan legislature introduced new laws in terms of the Computer Crimes Act No 24 of 2007.It mainly focuses on computer related crimes, hacking offences and content related Cyber Crimes. This paper focuses on the Cyber Crimes from a Sri Lankan perspective.

Computer Crime is classified under the criminal jurisdiction of the Act which is considered as a criminal statute. For a crime to occur there should be two components, namely, the act itself called the Actus Reus and the mind involved in committing the crime which is called the Mens Rea. A Computer Crime must satisfy both these criteria.

The Computer Crimes Act No 24 of 2007 identifies situations where this Act will apply, what is meant by a computer crime, how the crime is committed, how to identify the offenders and punishing the offenders. Cyber Crime is a major component of Computer Crimes and is tried through the internet media. This includes pornography, phishing, sexual harassments and email attacks. The Computer Crimes Act identifies such attacks and provides remedies to bring the offenders to the law.

RESEARCH QUESTIONS

1. To what extent of Cyber Crimes prevalent in Sri Lankan society?
2. To what extent the existing Computer Crime law is effective to combat such crimes?

THE OBJECTIVE

To focus on legislative measures the legislature has taken to combat Cyber Crimes in Sri Lanka.

SCOPE OF THE STUDY

Even though the Internet and computers are widely used in Sri Lanka the awareness among the general public with regard to hacking offences committed through this media is low. This research paper attempts to study the extent of Cyber Crimes prevalent in the Sri Lankan society by reviewing data published by the Sri Lanka Computer Emergency Response Team (SLCERT), the authorized national agency for cyber security and how the Cyber Crime legislation introduced through the Computer Crimes Act No 24 of 2007 could be utilized for redress.

METHODOLOGY

Methodology was mainly based on the literature research. This was carried out by reviewing the pilot case researches conducted by the Sri Lanka Computer Emergency Response Team (SLCERT) the authorized national agency and the review of legislations.

*All correspondence should be addressed to Ms. M. K. Goonathilaka, Department of Legal Studies, Open University of Sri Lanka (email: kusalaousl@yahoo.com)

DISCUSSION

Ever increasing trends of these crimes have been observed both in developed and developing countries. Though Sri Lanka is no exception to this trend only the tip of the ice berg is seen due to poor reporting mainly due to unawareness.

Among Cyber Crimes Phishing is a very popular Cyber Crime in which is the act of sending an email falsely claiming to be an established legitimate business where the unsuspecting recipient divulges personal, sensitive information such as passwords, credit card numbers, and bank account information and details. Here the unsuspecting client divulges these to a falsely website which the hackers operate. Data published by the SLCERT states that the most common Cyber Crime is the Sexual Harassments by publishing information without consent on the Internet. Other Cyber Crimes that are reported is Pornography and the unwanted mails in which the internet users face harassment as "Spam Mails".

Introduction of the Computer Crimes Act No 24 of 2007 has legally addressed the ways and means of combating Cyber Crimes. This is carried out through investigations and appointing a team of specialized investigators. Computer Crimes Act gives authority to investigate such crimes and identified and specified special investigation procedures and given authority to investigate in its due paragraphs.

Establishment of a computer emergency response team is a positive step towards combating these crimes and in Sri Lanka this is called SLCERT to overcome cyber attacks. This had been carried out through the Computer Crime legislature. It is the Center for cyber security in Sri Lanka and responses to cyber security threats and vulnerabilities.

Part 2 of the Act gives emphasis to investigation procedure relevant to offences. This is where the complaints, police investigations and search warrants are all identified and discussed. Sections 17, 17(3), 18 and 19 of the Computer Crimes Act 2007 are special important sections in relation to the investigations procedures.

Section 17 of the Act defined that appointment of a panel of experts for investigations and this was where the SLCERT had become its operation. Section 18 stated the powers of search of seizure with warrant in such an investigation. Section 19 of the Act defined the preservation of information in the investigation procedure.

According to the Section 17(3) of the Computer Crimes Act 2007 when carrying out the investigation an expertise of the field should be involved. Ideally expertise from Electronic Engineering or Software Technology was to be involved in the investigations.

Provisions applied for police officers also to involve in the investigation procedure and they are called as peace officers in such situations.

The Criminal Law of Sri Lanka applied where the Computer Crimes Act is silent on some issues and it stated that the prosecution to be carried out according to the provisions in the Code of Criminal Procedure when it was not specially mentioned.

In response to Cyber Crimes the authorized agency SLERT had carried out research in 2007.

In 2007 SLERT published statistics states that out of 17 cases reported 12% are for Hacking, 41% for Sexual Harassments (publishing information without consent) and 23% for impersonation.

According to SLCERT more than 160 Cyber Crimes complaints are reported as at 30/03/2011 and they are on hacking of passwords, stealing of information and demanding ransoms, facebook and credit cards related crimes.

CONCLUSIONS

This research focused on the Sri Lankan scenario of Cyber Crime attacks. It is concluded that with the increasing growth of Information Technology infrastructure in Sri Lanka, the cyber security breaches also had been increasing. Further research is necessary to identify parameters which would facilitate to identify different types of cyber security breaches which are not reported at this point of time with the existing methods available.

REFERENCES

Ian J. Lloyd and Maria J.Simpson(1996) Computer Crime, Computer Law Third Edition, Blackstone Press Ltd

Computer Crimes Act No 24 of 2007, Sri Lanka

http://www.cybercrime.gov , as at 30.03.2011

http://www.slcert.gov.lk , as at 30.03.2011